CLAIM LISTING:

1. (Currently Amended) A method for tracking the routing of an electronic document, comprising:

embedding a control mark, including a unique identifier and an encrypted check sum for authenticating the unique identifier, within a static section of an electronic document, wherein the static section remains unchanged when the electronic document is edited by a document editor; and

monitoring e-mail messages transmitted from senders to recipients, for detection of e-mail messages having the electronic document embedded therewithin or attached thereto, based on the unique identifier.

2. (Original) The method of claim **1** wherein the electronic document is a Microsoft Word document.

3. (Original) The method of claim **1** wherein the electronic document is a Microsoft Excel spreadsheet.

4. (Original) The method of claim **1** wherein the electronic documents is a Microsoft PowerPoint presentation.

5. (Original) The method of claim **1** wherein the electronic document is an Adobe PDF document.

6. (Original) The method of claim **1** wherein the electronic document is an HTML document.

7. (Original) The method of claim **1** wherein the electronic document is an XML document.

8. (Previously Presented) The method of claim **1** further comprising logging a recipient of an e-mail message having the electronic document embedded therewithin or attached thereto, in an audit record, when said monitoring detects the e-mail message, wherein the audit record stores information identifying a distribution route of the electronic document.

9. (Previously Presented) The method of claim **1** further comprising logging a sender of an e-mail message having the electronic document embedded therewithin or attached thereto, in an audit record, when said monitoring detects the e-mail message, wherein the audit record stores information identifying a distribution route of the electronic document.

10. (Previously Presented) The method of claim **1** further comprising logging a date and time of transmission of an e-mail message having the electronic document embedded therewithin or attached thereto, in an audit record, when said monitoring detects the e-mail message, wherein the audit record stores information identifying a distribution route of the electronic document.

11. (Previously Presented) The method of claim **1** further comprising generating a tracking report from audit records corresponding to at least one specified electronic document, wherein the audit records each stores information identifying a distribution route of the specified electronic document.

12. (Previously Presented) The method of claim **1** further comprising generating a tracking report from audit records corresponding to at least one specified user, wherein the audit records each stores information identifying a distribution route of an electronic document.

13. (Currently Amended) The method of claim **1** further comprising generating a tracking report from audit records corresponding to a specified time period, wherein the audit records each stores information identifying a distribution route of electronic documents ~~during~~.

14. (Previously Presented) The method of claim **1** further comprising logging a most recent file name of a file storing the electronic document, in an audit record, when said monitoring detects an e-mail message having the electronic document embedded therewithin or attached thereto, wherein the audit record stores information identifying a distribution route of the electronic document.

15. (Currently Amended) The method of claim **1** wherein said monitoring comprises authenticating the unique identifier using the encrypted check sum.

16. (Original) The method of claim **15** further comprising issuing a notification if said authenticating fails to authenticate the unique identifier.

17. (Original) The method of claim **1** further comprising:

examining an access control policy to determine whether or not permission is granted to transmit the electronic document to a recipient of an e-mail message having the electronic document embedded therewithin or attached thereto; and

causing transmission of the e-mail message to the recipient to be blocked, if said examining determines that permission is not granted.

18. (Original) The method of claim **17** further comprising issuing a notification about said causing to be blocked.

19. (Currently Amended) A system for tracking the routing of an electronic document, the system comprising one or more tangible computer-readable media collectively storing instructions encoding:

an auto-marking module for embedding a control mark, including a unique identifier and a check sum for authenticating the unique identifier, within a static section of an electronic document, wherein the static section remains unchanged when the electronic document is edited by a document editor; and

a traffic monitor for monitoring e-mail messages transmitted from senders to recipients, and for detecting e-mail messages having the electronic document embedded therewithin or attached thereto, based on the unique identifier.

20. (Original) The system of claim **19** wherein the electronic document is a Microsoft Word document.

21. (Original) The system of claim **19** wherein the electronic document is a Microsoft Excel spreadsheet.

22. (Original) The system of claim **19** wherein the electronic document is a Microsoft PowerPoint presentation.

23. (Original) The system of claim **19** wherein the electronic document is an Adobe PDF document.

24. (Original) The system of claim **19** wherein the electronic document is an HTML document.

25. (Original) The system of claim **19** wherein the electronic document is an XML document.

26. (Previously Presented) The system of claim **19** wherein the one or more media further store instructions encoding an auditor for logging a recipient of an e-mail message having the electronic document embedded therewithin or attached thereto, in an audit record, when said traffic monitor detects the e-mail message, wherein the audit record stores information identifying a distribution route of the electronic document.

27. (Previously Presented) The system of claim **19** wherein the one or more media further store instructions encoding an auditor for logging a sender of an e-mail message having the electronic document embedded therewithin or attached thereto, in an audit record, when said traffic monitor detects the e-mail message, wherein the audit record stores information identifying a distribution route of the electronic document.

28. (Previously Presented) The system of claim **19** wherein the one or more media further store instructions encoding an auditor for logging a date and time of transmission of an e-mail message having the electronic document embedded therewithin or attached thereto, in an audit record, when said traffic monitor detects the e-mail message, wherein the audit record stores information identifying a distribution route of the electronic document.

29. (Currently Amended) The system of claim **19** wherein the one [[ore]] or more media further store instructions encoding a reporter for generating a tracking report from audit records corresponding to at least one specified electronic document, wherein the audit records each stores information identifying a distribution route of the specified electronic document.

30. (Previously Presented) The system of claim **19** wherein the one or more media further store instructions encoding a reporter for generating a tracking report from audit records corresponding to at least one specified user, wherein the audit records each stores information identifying a distribution route of the electronic document.

31. (Previously Presented) The system of claim **19** wherein the one or more media further store instructions encoding a reporter for generating a tracking report from audit records corresponding to a specified time period, wherein the audit records each stores information identifying a distribution route of the electronic document.

32. (Currently Amended) The system of claim **19** wherein the one or more media further sore instructions encoding an auditor for logging [[the]] a most recent file name of a file storing the electronic document, in an audit record, when said traffic monitor detects an e-mail message having the electronic document embedded therewithin or attached thereto, wherein the audit record stores information identifying a distribution route of the electronic document.

33. (Currently Amended) The system of claim **19** wherein the one or more media further store instructions encoding a scanner for authenticating the unique identifier using the encrypted check sum.

34. (Currently Amended) The system of claim [[**19**]] 33 wherein the one or more media further store instructions encoding a notifier for issuing a notification if said ~~authenticating~~ scanner fails to authenticate the unique identifier.

35. (Previously Presented) The system of claim **19** wherein the one or more media further store instructions encoding:

a policy manager for examining an access control policy to determine whether or not permission is granted to transmit the electronic document to a recipient of an e-mail message having the electronic document embedded therewithin or attached thereto; and

a policy enforcer for causing transmission of the e-mail message to the recipient to be blocked, if said policy manager determines that permission is not granted.

36. (Previously Presented) The system of claim **35** wherein the one or more media further store instructions encoding a notifier for issuing a notification about said policy enforcer causing transmission of the e-mail message to be blocked.

37. (Canceled)

38. (Currently Amended) A method for tracking the routing of an electronic document, comprising:

embedding a control mark, including a unique identifier and an encrypted check sum for authenticating the unique identifier, within a static section of an electronic document, wherein the static section remains unchanged when the electronic document is edited by a document editor; and

monitoring transmitted network packets, for detection of network packets containing the electronic document, based on the unique identifier.

39. (Previously Presented) The method of claim **38** further comprising logging an audit record of the transmission, when a network packet containing the electronic document is detected by said monitoring, wherein the audit record stores information identifying a distribution route of the electronic document.

40. (Original) The method of claim **39** wherein said logging includes logging a date and time of the transmission in the audit record.

41. (Original) The method of claim **39** wherein said logging includes logging a destination of the transmission in the audit record.

42. (Currently Amended) The method of claim **38** wherein said monitoring monitors ~~networks~~ network packets transmitted internally within an organization network.

43. (Currently Amended) The method of claim **38** wherein said monitoring monitors ~~networks~~ network packets transmitted from within an organization network to outside of the organization network.

44. (Currently Amended) The method of claim **38** wherein said monitoring monitors ~~networks~~ network packets transmitted to an organization network from outside of the organization network.

45. (Original) The method of claim **38** wherein the network packets are transmitted in response to an FTP download.

46. (Original) The method of claim **38** wherein the network packets are transmitted in response to an HTTP download.

47. (Original) The method of claim **38** wherein the network packets are transmitted in response to an Instant Messenger download.

48. (Currently Amended) A system for tracking the routing of an electronic document, the system comprising one or more tangible computer readable media collectively storing instructions encoding:

an auto-marking module for embedding a control mark, including a unique identifier and a check sum for authenticating the unique identifier, within a static section of an electronic document, wherein the static section remains unchanged when the electronic document is edited by a document editor; and

a traffic monitor for monitoring transmitted network packets, and for detection of network packets containing the electronic document, based on the unique identifier.

49. (Previously Presented) The system of claim **48** wherein the one or more media further store instructions encoding an auditor for logging transmission information in an audit record when a network packet containing the electronic document is detected by said traffic monitor, wherein the audit record stores information identifying a distribution route of the electronic document.

50. (Previously Presented) The system of claim **49** wherein said auditor logs a date and time of the network packet's transmission in the audit record.

51. (Previously Presented) The system of claim **49** wherein said auditor logs a destination for the network packet in the audit record.

52. (Currently Amended) The system of claim **48** wherein said traffic monitor monitors ~~networks~~ network packets transmitted internally within an organization network.

53. (Currently Amended) The system of claim **48** wherein said traffic monitor monitors ~~networks~~ network packets transmitted from within an organization network to outside of the organization network.

54. (Currently Amended) The system of claim **48** wherein said traffic monitor monitors ~~networks~~ network packets transmitted to an organization network from outside of the organization network.

55. (Original) The system of claim **48** wherein the network packets are transmitted in response to an FTP download.

56. (Original) The system of claim **48** wherein the network packets are transmitted in response to an HTTP download.

57. (Original) The system of claim **48** wherein the network packets are transmitted in response to an Instant Messenger download.

58. (Canceled)

59. (Currently Amended) A method for controlling distribution of an electronic document within computer networks, comprising:

intercepting e-mail messages being transmitted from senders to recipients;

scanning the intercepted e-mail messages for detection of a specified electronic document embedded therein or attached thereto, wherein the specified electronic document includes a control mark within a static section thereof, wherein the control mark includes a unique identifier and an encrypted check sum for authenticating the unique identifier, and wherein the static section remains unchanged when the electronic documents is edited by a document editor;

examining a policy to determine whether or not transmission of the document to a recipient is permitted, if said scanning detects an e-mail message having the electronic document embedded therein or attached thereto; and

causing transmission of the document to the recipient to be blocked, if said examining determines that transmission is not permitted.

60. (Canceled)

61. (Original) The method of claim **59** wherein the policy indicates recipients permitted to access the electronic document.

62. (Original) The method of claim **59** wherein the policy indicates recipients not permitted to access the electronic document.

63. (Original) The method of claim **59** wherein the policy indicates senders permitted to send the electronic document.

64. (Original) The method of claim **59** wherein the policy indicates senders not permitted to send the electronic document.

65. (Original) The method of claim **59** further comprising issuing a notification, if said examining determines that transmission is not permitted.

66. (Previously Presented) The method of claim **59** further comprising generating an audit record to record transmission of the electronic document via an e-mail message, if said examining determines that transmission is permitted, wherein the audit record stores information identifying a distribution route of the electronic document.

67. (Currently Amended) A system for controlling distribution of an electronic document within computer networks, the system comprising one or more tangible computer-readable media collectively storing instructions encoding:

a traffic monitor for intercepting e-mail messages being transmitted from senders to recipients;

a scanner for scanning the intercepted e-mail messages, and for detecting a specified electronic document embedded therein or attached thereto, wherein the specified electronic document includes a control mark within a static section thereof, wherein the control mark includes a unique identifier and an encrypted check sum for authenticating the unique identifier, and wherein the static section remains unchanged when the electronic documents is edited by a document editor;

a policy manager for examining a policy to determine whether or not transmission of the specified electronic document to a recipient of an e-mail message is permitted; and

a policy enforcer for causing transmission of the specified electronic document to the recipient to be blocked.

68. (Canceled)

69. (Original) The system of claim **67** wherein the policy indicates recipients permitted to access the electronic document.

70. (Original) The system of claim **67** wherein the policy indicates recipients not permitted to access the electronic document.

71. (Original) The system of claim **67** wherein the policy indicates senders permitted to send the electronic document.

72. (Original) The system of claim **67** wherein the policy indicates senders not permitted to send the electronic document.

73. (Previously Presented) The system of claim **67** wherein the one or more media further store instructions encoding a notifier for issuing a notification, if said examining determines that transmission is not permitted.

74. (Previously Presented) The system of claim **67** wherein the one or more media further store instructions encoding an auditor for generating an audit record, to record transmission of the electronic document via an e-mail message, if said policy manager determines that transmission is permitted, wherein the audit record stores information identifying a distribution route of the electronic document.

75. (Canceled)

76. (Currently Amended) A method for controlling distribution of an electronic document within computer networks, comprising:

intercepting network packets transmitted over a computer network;

scanning the intercepted network packets for detection of network packets containing a specified electronic document, wherein the specified electronic document includes a control mark within a static section thereof, wherein the control mark includes a unique identifier and an encrypted check sum for authenticating the unique identifier, and wherein the static section remains unchanged when the electronic documents is edited by a document editor;

examining a policy to determine whether or not transmission of the specified electronic document is permitted, if said scanning detects a network packet containing the specified electronic document; and

causing transmission of the document to be blocked, if said examining determines that transmission is not permitted.

77. (Canceled)

78. (Original) The method of claim **76** wherein the policy indicates recipients permitted to access the specified electronic document.

79. (Original) The method of claim **76** wherein the policy indicates recipients not permitted to access the specified electronic document.

80. (Original) The method of claim **76** wherein the network packets are transmitted in response to an FTP download.

81. (Original) The method of claim **76** wherein the network packets are transmitted in response to an HTTP download.

82. (Original) The method of claim **76** wherein the network packets are transmitted in response to an Instant Messenger download.

83. (Currently Amended) A system for controlling distribution of an electronic document within computer networks, the system comprising one or more tangible computer-readable media collectively storing instructions encoding:

a traffic monitor for intercepting network packets transmitted over a computer network;

a scanner for scanning the intercepted network packets and for detecting network packets containing a specified electronic document, wherein the specified electronic document includes a control mark within a static section thereof, wherein the control mark includes a unique identifier and an encrypted check sum for authenticating the unique identifier, and wherein the static section remains unchanged when the electronic documents is edited by a document editor;

a policy manager for examining a policy to determine whether or not transmission of the specified electronic document is permitted; and

a policy enforcer for causing transmission of the specified electronic document to be blocked.

84. (Canceled)

85. (Original) The system of claim **83** wherein the policy indicates recipients permitted to access the specified electronic document.

86. (Original) The system of claim **83** wherein the policy indicates recipients not permitted to access the specified electronic document.

87. (Original) The system of claim **83** wherein the network packets are transmitted in response to an FTP download.

88. (Original) The system of claim **83** wherein the network packets are transmitted in response to an HTTP download.

89. (Original) The system of claim **83** wherein the network packets are transmitted in response to an Instant Messenger download.

90. (Canceled)